Lab 5
ECSE308 - Introduction to Communication Systems and Networks
Group C9

Ismail Faruk

Marine Huynh

Part 1: TCP

The ip address of the destination is 132.206.75.13.

1. How many TCP datagrams are exchanged between your computer and the server to establish the TCP connection? Why each of these segments is needed to setup the TCP connection?
6 datagrams were exchanged between the computer and the server. Each segment is needed to make sure that the connection has been established. The client sends a SYN to the server and it sends the segment's sequence to a random value A. In response, the server sends a SYN-ACK, which is an acknowledgement. The acknowledgement number is set to +1 of the random value A from SYN and the sequence number that the server chooses for the packet is another random number B. Then the clients sends an acknowledgement back to the server ACK. The acknowledgement number is increases by one.
In our case, the computer sent twice the packet, then the server acknowledged it. The computer tried to but failed so the server sent again the acknowledgement. The second time the computer received the acknowledgement, and the data was then passed.

2. Which end point started the TCP Connection-Establishment phase?
The client started the TCP Connection-Establishment phase.

3. What flags are set in each of these TCP datagrams?
The acknowledgement and syn flags are set for the TCP datagrams.

4. What is the initial value of the sequence number on the client's side?
The initial value of the sequence number on the client's side is 0.

5. What is the initial value of the sequence number on the server's side?
The initial value of the sequence number on the server's side is 0.

6. What is the value of the Acknowledgement field in the SYN ACK datagram? How did the server determine that value?
The value of the Acknowledgement in the SYN ACK is 1. The server checks if the flag has changed from 0 to 1, meaning 0 no acknowledgement, and 1 there is an acknowledgement.

7. For the TCP SYN datagram, determine the following:

8. the source port number - 62037

9. the destination port number - 80

10. the size of the window - 64240

11. the header length - 32 bytes

12. For the TCP SYN ACK datagram, determine the following:

13. the source port number - 80

14. the destination port number - 62037

15. the size of the window - 29200

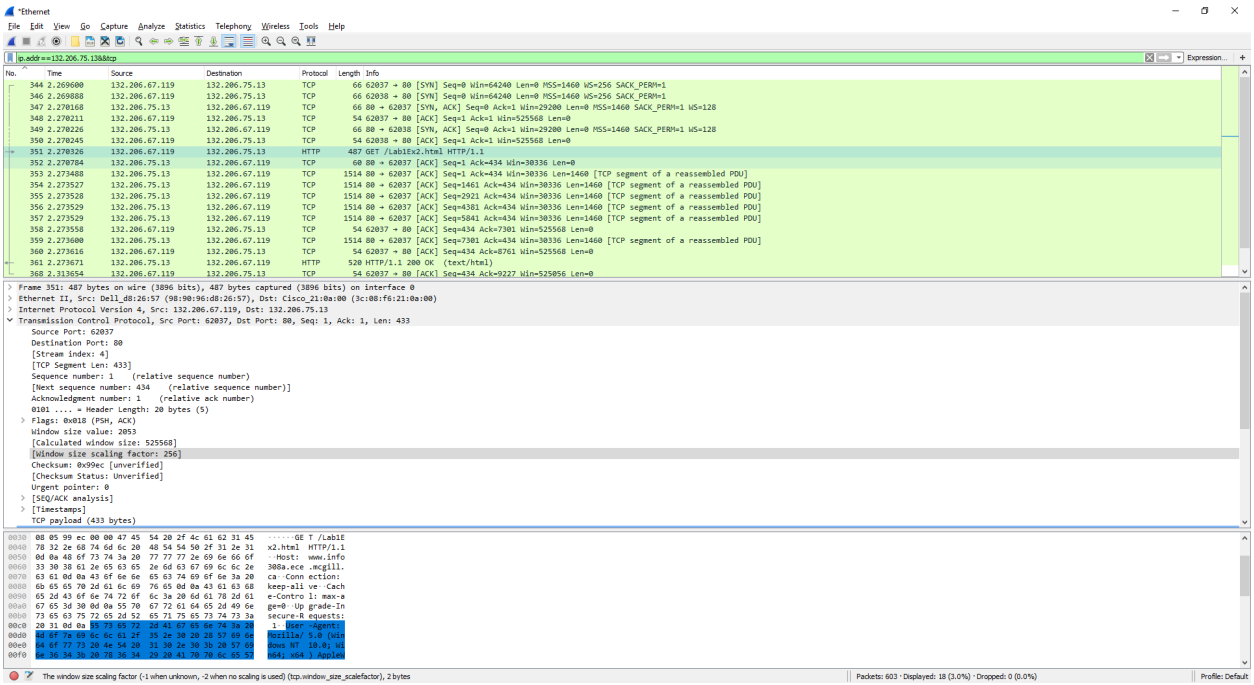
16. the header length - 32

17. What is the usage of the window field in the TCP segments?
The TCP window size field controls the flow of data and its value is limited to between 2 and 65,535 bytes.

18. Consider the TCP segment containing the HTTP GET as the first segment in the TCP connection. For the first three TCP segments, answer the following questions:

19. When was each segment sent?
Each segment was sent from 0.003888000 seconds.

20. At what time was the ACK for each segment received?
The ACK for each segment received after 0.003958000 seconds.



Part 2: HTTP

I. Simple HTTP get method

30. What HTTP request method is used to retrieve the HTML file?
The get method is used to retrieve the HTML file.

31. What is the URI of the requested file?
The URI of the requested file is /Lab1Ex1.html

32. What HTTP version is your browser running? What are the other versions of HTTP?
The HTTP version of our browser is HTTP/1.1. Other versions of HTTP exists such as HTTP/2.

33. What languages does your browser accept for response?
Our browser accepts languages :en-US,en;q=0.9\r\n.

34. What is the IP address of your computer?
The IP address of our computer is 132.206.67.119.

35. What is the server's IP address?
The server IP address is 132.206.75.13.

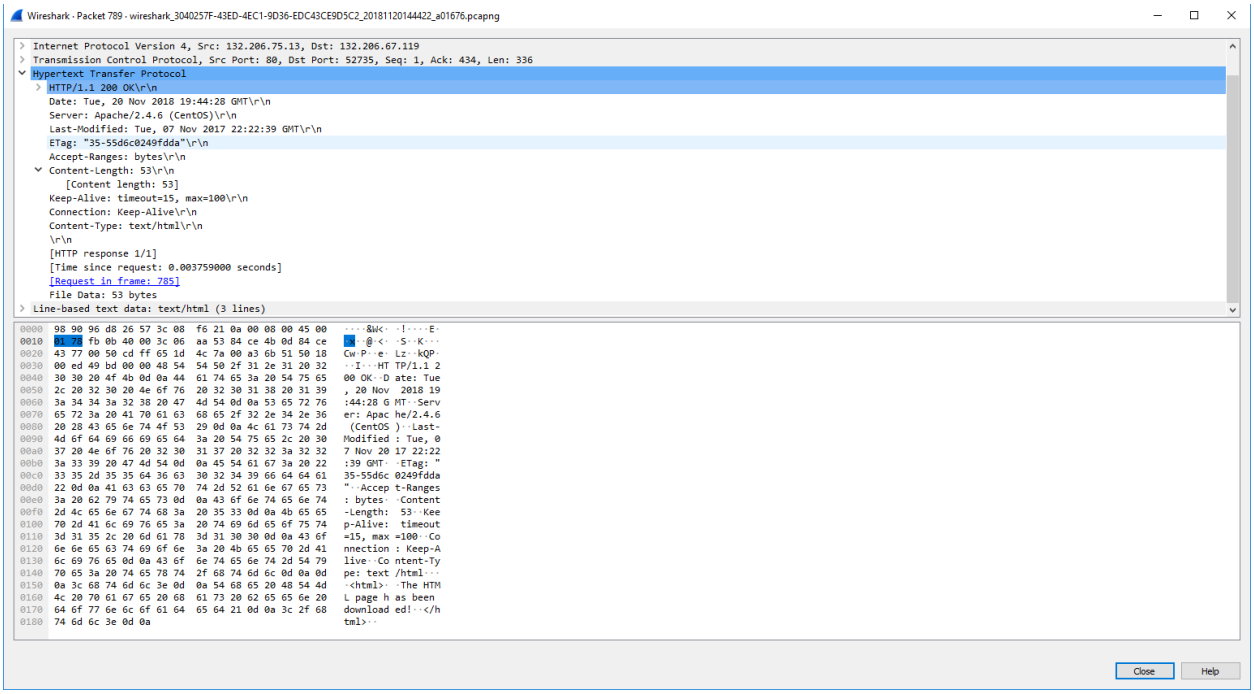
36. What is the relationship between source and destination IP addresses of the first GET and the source and destination IP addresses of the first response?

The source IP address of the GET is the destination IP address of the first response.
The destination IP address of the GET is the source IP address of the first response.

37. What is the status code of the first response message? What does this code indicate? What code is returned if the requested file cannot be found on the server?
The status code of the first response message is a code 200. This means “OK”, as in the response is successful. If the request could not be completed because it could not find a file on the server, then the status code is 404, meaning “Not Found”.

38. When was the last time that the received HTML file was modified at the server?
The last modified date is Tue, 07 Nov 2017 22:22:39 GMT.

39. What is the size of the content that is returned to your browser?
The size of the content returned was 53 bytes.



II: Long HTTP

40. How many HTTP GET request messages are sent by your web browser?
One HTTP GET request is sent.

41. By inspecting the entire trace, determine the number of packets that contain HTTP header. Explain your answer.

The HTTP header contains 2 packets. One packet was the GET and the other packet was the response from server.

42. How many TCP segments are transmitted to your computer? Why multiple segments are required to retrieve this single HTML file?
There are 7 TCP segments transmitted. There are multiple segments because the message is too long for TCP to transmit correctly. Therefore, it breaks the data into smaller segments to pass them, and it will reconstruct at the end to retrieve the message sent.

43. Determine the length of these TCP segments. Do they have the same size? Explain your answer.
The total TCP length is 9226 bytes. The first 6 segments have each a length of 1460 bytes and the last segments has length 466 bytes. The maximum size of a segment is 1460, which is why we have 6 full segments, and the 7th one contains the remaining bytes to send the full message.

44. Which message and what field in that message indicate that the server was able to process the request successfully?
The HTTP status code sent is an "acknowledgement" of how the request went. The code was 200, which means that it is ok. In other cases, where the website would not be found a code such as 404 could be sent.

III: HTTP Caching

45. What is the status code of the first response message?
The status code of the first response message is 200.

46. What is the value of the content size of the first response message?
The content length is 384 bytes.

47. What is the etag (identity tag) of the first response message?
The etag of the first response message is "180-55d56212e3419".

48. What is the application of etag in conditional HTTP request? Which line in the second response contains the etag value of the first response?
The ETag or entity tag is part of HTTP, the protocol for the World Wide Web. It is one of several mechanisms that HTTP provides for web cache validation, which allows a client to make conditional requests. The Etag line in the second response contains the Etag "180-55d56212e3419".

49. Which HTTP GET contains the "IF-MODIFIED-SINCE" line? What is the usage of this field?

The second HTTP get contains the “IF-MODIFIED-SINCE” line. The usage of this field is to know if the get method on this url was already accessed once and is now stored in the cache. This allows for fast access so it does not require to go further to retrieve information for the page, such as css or xml files. The If-Modified-Since request HTTP header makes the request conditional: the server will send back the requested resource, with a 200 status, only if it has been last modified after the given date. If the request has not been modified since, the response will be a 304 without any body.

50. What is the status code of the second response message? What does this code mean?
Status code of the second response is 304. This code means “Not modified”.

51. What is the content length of the second response? Explain.
Content length of the second response is 0, because the content was already received in the first response and the second response did not contain any content, as the content already existed in the browser cookies.

IV: Retrieving a web page

52. How many HTTP GET requests are sent by your web browser?
Our browser sent 2 HTTP GET requests.

53. What is the content type of each response message?
The first response contained text/html.
The second response contained image/png.

54. Did your browser download the two images serially or in parallel? Explain. What are the pros and cons of each approach?
The browser downloaded the two images in serial, because the first image must have been done first by wikipedia before the second can get onto it from ieee. We can also see that the second get method only downloads the second image. Therefore, they must have been done one after the other.

55. Has the HTTP used persistent or non-persistent connection? Explain your answer.
The HTTP uses persistent connection, because it is HTTP/1.1, which is persistent connection by default. It also has Connection: Keep-Alive.

V: HTTP request methods

56. What is the requested URL in the frame#101? What HTTP field contains the username and password information? What are the submitted values for the username and the password?
The frame #101 is the first get method. There are no username and password.

57. What HTTP request method is used in the frame#172? What HTTP field contains the username and password information? Explain the difference between this request method and the GET method.
The frame #172 is done with a post method. This sends information and does not expect a response. GET method retrieves the answer.

58. What is the status code of the frame#174? What is the description of this code?
The frame #174 is the response with its status code 200, which means that it was successful.